DATE(S) ISSUED:
12/11/2013

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- · Firefox versions prior to 26.0
- · Firefox Extended Support Release (ESR) versions prior to 24.2
- · Thunderbird versions prior to 24.2
- · SeaMonkey versions prior to 2.23

RISK:
Government:
- · Large and medium government entities: **High**
- · Small government entities: **High**

Businesses:
- · Large and medium business entities: **High**
- · Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

- · Mozilla Firefox, Thunderbird and SeaMonkey are prone to a security-bypass vulnerability because trust settings for built-in roots are ignored during Extended Validation(EV) certificate validation. Specifically, this issue occurs because EV root certificates are trusted even if the user has explicitly removed their trust. [CVE-2013-6673] [MFSA 2013-113]
- · Mozilla Firefox, Thunderbird, and SeaMonkey are prone to multiple unspecified memory-corruption vulnerabilities that exist in the browser engine. [CVE-2013-5610] [CVE-2013-5609] [MFSA 2013-104]

- Mozilla Firefox and SeaMonkey are prone to an information-disclosure vulnerability because it fails to properly restrict the web content from accessing the data saved to the clipboard. Specifically, the issue exists when a user attempts to paste a selection with a middle-click instead of pasting the selection content. [CVE-2013-6672] [MFSA 2013-112]
- Mozilla Firefox, Thunderbird and SeaMonkey are prone to a memory-corruption vulnerabiliy due to a heap-use-after-free error when interacting with event listeners from the 'mListeners' array. Specifically, this issue affects the 'libxul.so!nsEventListenerManager::HandleEventSubType()' function. [CVE-2013-5616] [MFSA 2013-108]
- Mozilla Firefox and Seamonkey are prone to a security-bypass vulnerability that occurs because the '<iframe sandbox>' restrictions are not applied to an '<object>' element contained within a sandboxed iframe. [CVE-2013-5614] [MFSA 2013-107]
- Mozilla Firefox, Thunderbird and SeaMonkey are prone to multiple memory-corruption vulnerabilities due to a heap-use-after-free error. Specifically, this issue affects the 'libxul.so!PresShell::DispatchSynthMouseMove()' function. [CVE-2013-5613] [MFSA 2013-114]
- Mozilla Firefox is prone to a security-bypass vulnerability because the doorhanger notification for Web App installation may persist from one site to another without being dismissed by the navigation. Attackers can exploit this issue to trick an unsuspecting user into installing an application from one site while seemingly to come from trusted site. [CVE-2013-5611] [MFSA 2013-105]
- Mozilla Firefox, SeaMonkey, and Thunderbird are prone to a remote code-execution vulnerability due to a segmentation fault in the libxul.so!nsGfxScrollFrameInner::IsLTR()' function when inserting an ordered list into a document through script. [CVE-2013-6671] [MFSA 2013-111]
- Mozilla Firefox and SeaMonkey are prone to a memory-corruption vulnerability due to an overflow in the binary search algorithms of the SpiderMonkey javascript engine. [CVE-2013-5619] [MFSA 2013-110]
- Mozilla Firefox, Thunderbird and SeaMonkey are prone to multiple memory-corruption vulnerabilities due to a heap-use-after-free error. Specifically, this issue affects the 'nsNodeUtils::LastRelease()' on anonymous node from 'ShowInlineTableEditingUI()' function.   [CVE-2013-5618] [MFSA 2013-109]
- Mozilla Firefox, Thunderbird and SeaMonkey are prone to a cross site scripting vulnerability due to an issue related to inherited character set encoding information. [CVE-2013-5612] [MSFA 2013-106]
- Mozilla Firefox, Thunderbird and SeaMonkey are prone to a security vulnerability due to an error when generating GetElementIC typed array stubs outside observed typesets during JavaScript compilation. [CVE-2013-5615] [MSFA 2013-115]

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data, or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
Mozilla:
http://www.mozilla.org/security/announce/2013/mfsa2013-104.html
http://www.mozilla.org/security/announce/2013/mfsa2013-105.html
http://www.mozilla.org/security/announce/2013/mfsa2013-106.html
http://www.mozilla.org/security/announce/2013/mfsa2013-107.html
http://www.mozilla.org/security/announce/2013/mfsa2013-108.html
http://www.mozilla.org/security/announce/2013/mfsa2013-109.html
http://www.mozilla.org/security/announce/2013/mfsa2013-110.html
http://www.mozilla.org/security/announce/2013/mfsa2013-111.html
http://www.mozilla.org/security/announce/2013/mfsa2013-112.html
http://www.mozilla.org/security/announce/2013/mfsa2013-113.html
http://www.mozilla.org/security/announce/2013/mfsa2013-114.html
http://www.mozilla.org/security/announce/2013/mfsa2013-115.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6673
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5609
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5610
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6672
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5616
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5614
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5613
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5611
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6671
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5618
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5619
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5612
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5615

SecurityFocus:
http://www.securityfocus.com/bid/64213
http://www.securityfocus.com/bid/64206
http://www.securityfocus.com/bid/64204
http://www.securityfocus.com/bid/64210
http://www.securityfocus.com/bid/64209
http://www.securityfocus.com/bid/64207
http://www.securityfocus.com/bid/64203
http://www.securityfocus.com/bid/64214
http://www.securityfocus.com/bid/64212
http://www.securityfocus.com/bid/64215
http://www.securityfocus.com/bid/64211
http://www.securityfocus.com/bid/64206
http://www.securityfocus.com/bid/64216